

(2026년도 상반기)

정보보호 전문가를 위한 암호교육

| 기 간 | 2026년 6월 29일(월)~7월 10일(금)

| 장 소 | 온라인 교육

| 주 최 | 한국암호포럼, 한국정보보호학회

| 주 관 | 한국암호포럼

| 프로그램 위원장 |

서석충 교수(국민대학교), 박명서 교수(한성대학교)

| 프로그램 위 원 |

김영식 교수 (DGIST) 송용수 교수(서울대)
이주희 교수 (성신여대)

■ 교육비

구 분	교 육 비
학 생 / 일 반	30 만원 / 50 만원

■ 온라인 등록

- 사전등록 : 2026년 06월 26일(금)까지
- 기타사항 : 1) 교육 증명서 발급
2) 온라인 접속 링크 등록자 개별 공지
- 등록방법 : 학회홈페이지(<https://www.kiisc.or.kr>)
→ 학회행사 → 사전등록바로가기
- 결 재 방 법 : 등록정보 작성 후 결제방법 선택 및 결제

| 등 록 안 내 |

■ 사전 등록 송금처

- 예 금 주 : 한국정보보호학회
- 계좌번호 : 국민은행 754201-04-135596
(예금주: 한국정보보호학회)
- 안내사항 : 1) 사전등록시 등록비는 위의 계좌로
송금하시고, 입금자가 대리일 경우
연락바람
2) 신용카드 결제시 세금계산서 발급 불가
(부가가치세법 시행령 제 57조)

■ 문의처 : 한국정보보호학회

- 전 화 : 02-564-9333~4 (내선번호 0)
- 전자우편 : kiisc@kiisc.or.kr

교육 일정

날 짜	주제	강 의 제 목	강 사
6월 29일 (월) ~ 7월 10일 (금)	격자기반 암호	1.1 격자기반암호 배경 지식 및 격자 기본 이론	이주희 교수 (성신여대)
		1.2 격자기반 공개키 암호 및 KEM	
		1.3 격자기반 전자서명	
	동형암호	2.1 동형암호 개요	송용수 교수 (서울대)
		2.2 동형암호 구조 및 스킴 소개	
		2.3 동형암호 최신 연구 방향	
	코드기반 암호	3.1 부호이론 소개	김영식 교수 (DGIST)
		3.2 McEliece 코드 암호 소개 및 코드기반암호 분석 동향	
		3.3 NIST PQC 공모전 4라운드 코드기반암호 소개	

교육 개요

○ PART 1. 격자기반암호

강사	이주희 교수 (성신여자대학교)
약력	2019년: 서울대학교 이학박사 2019년~2022년: 삼성SDS 연구원 2022년~현재: 성신여자대학교 융합보안공학과 교수
E-mail	jooheelee@sungshin.ac.kr

제목	1.1. 격자기반암호 배경 지식 및 격자 기본 이론
내용	- 수학적 배경 - 격자 이론

제목	1.2. 격자기반 공개키 암호 및 KEM
내용	- Learning with Errors - LWE-based Encryption - CRYSTALS-Kyber (ML-KEM)

제목	1.3. 격자기반 전자서명
내용	- Schnorr Signature - Lattice-based Signature - CRYSTALS-Dilithium (ML-DSA)

○ PART 2. 동형암호

강 사	송용수 교수 (서울대학교)
약 력	2018년: 서울대학교 이학박사 2018년: UC San Diego 박사후연구원 2019년~2021년: Microsoft Research 선임연구원 2021년~현재: 서울대학교 컴퓨터공학부 교수
E-mail	y.song@snu.ac.kr

제 목	2.1. 동형암호 개요
내 용	- 동형암호 배경 - 동형암호 연구 히스토리

제 목	2.2. 동형암호 구조 및 스킴 소개
내 용	- LWE와 RLWE 기반 문제 - BFV 스킴 - CKKS 스킴

제 목	2.3. 동형암호 최신 연구 방향
내 용	- 연구적 도전과제 - 미래 연구 방향성

○ PART 3. 코드기반 암호

강 사	김영식 교수 (DGIST)
약 력	2007년: 서울대학교 공학박사 2007년~2010년: 삼성전자 선임연구원 2010년~2023년: 조선대학교 정보통신공학과 교수 2023년~현재: DGIST 전기전자컴퓨터공학과 교수
E-mail	ysk@dgist.ac.kr

제 목	3.1. 부호이론 소개
내 용	- 선형블록코드 소개 - 코드기반 암호 개요

제 목	3.2. McEliece 코드 암호 소개 및 코드기반암호 분석 동향
내 용	- McEliece 기본 설계 방향 소개 - McEliece 세부 연산 소개 (키쌍생성, 암호화, 복호화) - 코드기반암호 안전성 분석 동향 소개

제 목	3.3. NIST PQC 공모전 4라운드 코드기반암호 소개
내 용	- Classic McEliece 암호 소개 - BIKE 암호 소개 - HQC 암호 소개